

Curs 9

Structuri Algebraice în Informatică

Ideale. Inele factor.

Teorema fundamentală de izomorfism

$n \in \mathbb{N}^*$ ~ am lucrat cu clasele de resturi modulo $n \rightsquigarrow (\mathbb{Z}_n, +, \cdot)$ inel comutativ

sat $f \in A[x]$ polinom de grad n monic

\rightsquigarrow am lucrat cu clase de resturi modulo

$f \rightsquigarrow (A[x]/(f), +, \cdot)$ inel

$\forall x \in A[x], g_1 \equiv g_2 \pmod{f}$ dacă $f' \mid g_1 - g_2$

a dică $g_1 \sim g_2 = f \cdot k$ cu $k \in A[x]$

Vrem să extindem lucrul cu "clase de resturi" din \mathbb{Z} la lucrul cu "clase de resturi modulo" un multime mai largă de elemente dintr-un inel I

modulo un ideal $[n, f]$

în felul căor $[(\mathbb{Z}_m, +, \cdot)], (A[x]/(f), +, \cdot)]$

În continuare $(A, +, \cdot)$ inel comutativ

$(\mathbb{Z}, \mathbb{Z}_m, \mathbb{Q}, \mathbb{R}, \dots, \mathbb{Z}[x], \dots, K[x], \dots)$

Def: O submultime nuempty a集ăorii A se numește ideal în A dacă și:

$$(1) \forall x, y \in J, x + y \in J$$

$$(2) \forall a \in A, \forall x \in J, ax \in J$$

Prop: $J \subseteq A$ este ideal în $A \Leftrightarrow$

$$\forall x_1, x_2 \in J \quad x_1 + x_2 \in J$$

$$\forall a_1, a_2 \in J \quad a_1 x_1 + a_2 x_2 \in J$$

"n combinatia liniară"

Dcm, \Rightarrow "Pp" J satisfac (1) și (2) din def.

$$a_1 \in A \ni x_1 \in J \stackrel{(2)}{\Rightarrow} a_1 x_1 \in J$$

$$a_2 \in A \ni x_2 \in J \stackrel{(2)}{\Rightarrow} a_2 x_2 \in J$$

$$\Rightarrow a_1 x_1 + a_2 x_2 \in J$$

$$x, y \in J, x - y = x + (-y) \in J$$

$$a \in A \ni x \in J, ax = a(x - y) + a(y) \in J$$

Obo! 1) dacă J ideal $\Rightarrow 0 \in J$

$$J \neq \emptyset \rightarrow 0 = 0 \cdot x \in J$$

2) În def. putem înlocui cond (1) cu

$$(1'): \forall x, y \in J, x - y \in J$$

Deci un ideal este un subgrup cu "+"

3) O intersecție arbitrară de ideale este un ideal în acel inel

4) $\{0\}$ și A sunt ideale în θ

5) Dacă un ideal J avem $J \cdot A \in J \cap U(A) \neq \emptyset$

6) $1 \in J$ $\underline{(3)}$

6) Un corp K are doar două ideale $\{0\}$ și K

Dacă $J \neq \{0\} \Rightarrow J \subseteq eJ$, deci $eJ = K$
 $J \cap U(K) = \emptyset$, deci $J = K$

Teorema / Definiție: Fie A inel comutativ

$\exists S \subseteq A$ submultime

astfel încât $\bigcap_{I \in \mathcal{I}} I$ este cel mai mic ideal

ideal din $\mathcal{I}(S)$

(în sensul inclusiunii), dim A nu conține multă multă S .

0 $\bigcap_{I \in \mathcal{I}(S)} I$ se numește idealul generat de S în A .

În plus, dacă $S = \emptyset$, $(\emptyset) = \{0\}$

dacă $S \neq \emptyset$, $(S) = \{a_1x_1 + \dots + a_nx_n : n \in \mathbb{N}, a_1, \dots, a_n \in S\}$

$n \in \mathbb{N}, a_1, \dots, a_n \in S$

$a_1, \dots, a_n \in S$

Sănsem că un ideal J este finit generat doar și să fie finit $\Leftrightarrow J = (S)$.

- II - este ideal principal dacă poate

fi generat de un singur element:

$$\exists x \in J \text{ cu } J = (x)$$

$$\text{Ex: } (x) = \{ax \mid a \in A\} = Ax$$

\hookrightarrow ideal generat de un element \rightarrow multipli aceluiași element

$$(x_1, x_2, \dots, x_m) = \left\{ \sum_{i=1}^m a_i x_i \mid a_i \in A, i = 1, m \right\} =$$

$$= \sum_{i=1}^m Ax_i$$

Teorema $\exists m$ inelile $\mathbb{Z}, \mathbb{Z}_m, K[x]$ cu K corp, oricărui ideal este principal

Dem. Cazul \mathbb{Z} : zilei J ideal în \mathbb{Z} . Dacă

$$J = \{0\} = (0), \text{ deci ideal principal}$$

$$\text{Pp că } J \neq \{0\} \Rightarrow \exists x \in J \Leftrightarrow x \in J$$

(J subgrup în $(\mathbb{Z}, +)$)

Notăm $x = \min(\mathbb{N}^* \cap J) \neq \emptyset$. Astătămcă
 $J = (x) \quad | \quad x \in J \Rightarrow \forall a \in \mathbb{Z}, a \cdot x \in J \Rightarrow (x) \subseteq J$

P.p. $\exists y \in J \setminus \{x\} \Rightarrow$ dacă împărțim

cu rest r la x , $y = qx+r$, over $r \neq 0$

$r = y^{e_j} - g x^{e_j} \in J$ fals (x este mai mic) \Rightarrow

$\Rightarrow J = (x)$: ideal primar

Prop: considerăm $A = \mathbb{Z}$ sau $A = K[x]$ cu K corp.

Avem $f_1, f_2, \dots, f_m \in A$ astfel că $(f_1, \dots, f_m) = (\gcd(f_1, \dots, f_m))$

$$(f_1) \cap (f_2) \cap \dots \cap (f_m) = (\text{lcm}(f_1, \dots, f_m))$$

Bază Primă inducție după m

$$m=1 \vee$$

$$m=2: (f_1, f_2) = \{a f_1 + b f_2 \mid a, b \in \mathbb{Z}\} = \overline{\gcd(f_1, f_2)}$$

idealul generat de $a, b \in \mathbb{Z}$ în $A = \mathbb{Z}$:

generatorul este cel mai mic $m > 0$ de forma $a f_1 + b f_2$ cu $a, b \in \mathbb{Z}$

deci $\gcd(f_1, f_2)$

Pasul de inducție

$$(f_1, \dots, f_{m+1}) = ((f_1, \dots, f_m), f_{m+1})$$

$$= (\gcd(f_1, \dots, f_m), f_{m+1})$$

$$= (\gcd(f_1, \dots, f_m))$$

Avem $f \in (f_1) \cap \dots \cap (f_m) \Leftrightarrow f \in (f_i) \forall i \in \{1, \dots, m\}$

$\Leftrightarrow f_i \mid f \forall i = 1, \dots, m \Leftrightarrow \text{lcm}(f_1, \dots, f_m) \mid f \Leftrightarrow$

$f \in (\text{lcm}(f_1, \dots, f_m))$

Inelul factor

Fie J un ideal în inelul comutativ.
Pe A definim relația de congruență modulo J :
 $\forall x, y \in A \quad x \equiv y \pmod{J} \text{ dacă } x - y \in J$
 $(\text{mod } x \sim y \text{ și})$

Proprietăți

1) \sim este o relație echivalență pe A

$$(R): \forall x \in A \quad x - x = 0 \in J \Rightarrow x \sim x$$

$$(S): \forall x, y \in A \quad x - y \in J \Rightarrow -(x - y) \in J \Rightarrow$$

$$\Rightarrow y - x \in J \Rightarrow y \sim x$$

$$(D): \forall x, y, z \in A \quad \text{dacă } x \sim y \text{ și } y \sim z \Rightarrow x \sim z$$

$$\Rightarrow x \sim y \sim z$$

2) $\forall z \in J$, dacă $x \sim y$, atunci $x + z \sim y + z$

$$x + z \sim y + z$$

3) $\forall q \in A, Q = \{b \in A \mid b - q \in J\} = q + J$

clasa de echivalență

Spatială cu tot x not: $A/x = \{a \in A \mid a \sim x\}$

4) $\hat{a} = \hat{0} \Leftrightarrow a - 0 \in J \Leftrightarrow a \in J$

5) Pe A/x definim și operații

$\hat{x} + \hat{y} = \hat{x} + \hat{y}$ nu depinde de reprez.
 $\hat{x} \cdot \hat{y} = \hat{x} \hat{y}$ astăzi și obținem $(A/y, \cdot)$
 este un inel comutativ
 numit inelul factor
 și modulo J .

ō element neutru 1_A , $\hat{1}_J$

ī el. neutru 0_A , $\hat{0}_J$

pt $a \in J$, $\hat{a} = 0$

Teoremul de corespondență: J o corespondență
 bijectivă multe idealele lui A cu contin mărginim J

→ idealele dim A/y

$$y_1 \supseteq J \longrightarrow J_1 / y \subseteq A/y$$

Dacă $f: A_1 \rightarrow A_2$ este un morfism de
 inele, numim nucleul lui f $\text{Ker } f = \{x \in A_1 \mid f(x) = 0\}$ nucleus morfismului f (kernel)

Obs! Dacă J ideal și inelul A

funcția $\pi: A \rightarrow A/y$ este un morfism
 surjectiv $x \mapsto x + J$

d. inele cu $\text{Ker } \pi = J$

Teoremul fundamental de izomorfism în inele

Fie $f: A_1 \rightarrow A_2$ un morfism de inele. Atunci
 există un ideal în A_1 și funcția
 $\tilde{f}: A_1 / \text{ker}(f) \rightarrow \text{Im}(A_2)$ este un
 izomorfism

$x \mapsto f(x)$ sau $[A/\ker f = \text{Im } f]$

Exemplu: 1) pt $n \in \mathbb{N}^+$, $\{m = h^{n-k} \mid k \in \mathbb{Z}\}$
înmulțitorul $\mathbb{Z}/(n)$ este de formă $= \text{mod}_n$
este $(2n, +, \cdot)$

2) K corp comutativ și $f \in K[x]$ de
(sau înel)
grad n
(monic)

$$(f) = \{f \cdot h \mid h \in K[x]\}$$

$$g_1 \sim_{(f)} g_2 \Leftrightarrow g_1 - g_2 \in (f) \Leftrightarrow f | g_1 - g_2 \Leftrightarrow$$

$$\Leftrightarrow g_1 = g_2 \pmod{f}$$

Înmulțitorul $K[x]/(f)$ este de formă
înmulțitorul de resturi modulo f